SUPERIOR COURT OF THE DISTRICT OF COLUMBIA

CRIMINAL DIVISION – FELONY BRANCH

In the Matter of the Search of	**)**	**Special Proceeding No. 17 CSW 3438**
www.disruptj20.org that Is Stored at	**)**	
Premises Owned, Maintained, Controlled, or	**)**	**Judge Leibovitz**
Operated by DreamHost	**)**	**Hearing: 9:30 a.m. Friday, Aug. 18, 2017**
	)	
_____/		

NON-PARTY DREAMHOST, LLC'S RESPONSE IN OPPOSITION TO UNITED STATES' MOTION FOR DREAMHOST TO SHOW CAUSE

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes

Other Authorities

I. Introduction

Where a search warrant endangers First Amendment interests, the warrant must be scrutinized with "particular exactitude" under the Fourth Amendment. See Zurcher v. Stanford Daily, 436 U.S. 547, 565 (1978). "The First Amendment is often inconvenient. But that is beside the point. Inconvenience does not absolve the government of its obligation to tolerate speech." Int'l Soc'y for Krishna Consciousness, Inc. v. Lee, 505 U.S. 672, 701 (1992) (Kennedy, J., concurring). The government's search warrant ("Search Warrant") here requires non-party DreamHost, LLC ("DreamHost") to turn over every piece of information it has about every visitor to a website expressing political views concerning the current administration. This information includes the IP address for the visitor, the website pages viewed by the visitor, even a detailed description of software running in the visitor's computer. In essence, the Search Warrant not only aims to identify the political dissidents of the current administration, but attempts to identify and understand what content each of these dissidents viewed on the website. The Search Warrant also includes a demand that DreamHost disclose the content of all e-mail inquiries and comments submitted from numerous private e-mail accounts and prompted by the website, all through a single sweeping warrant.

The Search Warrant cannot survive scrutiny under the heightened particular exactitude standard required by the presence of the First Amendment issues. It fails to identify with the required particularity what will be seized by the government. It also fails to provide DreamHost with any assurance that the government will return or destroy the large portion of the information irrelevant to the government's criminal case or cases. These features render the Search Warrant unreasonable under the Fourth Amendment. In addition, the Search Warrant violates the privacy protections of the Privacy Protection Act, a statute enacted specifically to address such instances, and is without a jurisdictional basis.

II. Background

A review of the government's demands for information from DreamHost provides important context for DreamHost's objections to the Search Warrant.

A. The Government's January 27, 2017 Subpoena to DreamHost

Approximately one week after the 2017 U.S. Presidential Inauguration, the government provided DreamHost, a web hosting company, with a Grand Jury subpoena for records along with a request to preserve records. The subpoena called for seven categories of information concerning the DreamHost account using the internet domain name "disruptj20.org." Id. The categories in the subpoena included information identifying the individual registrant of the website, the registrant's physical addresses and e-mail addresses, information about the services the registrant obtained from DreamHost, the payment for those services, and information about the registrant's computer interactions with DreamHost's servers. Id.

Within three weeks of service of the subpoena, DreamHost produced its records responsive to these categories. In its correspondence accompanying the production, DreamHost's General Counsel made clear that he understood the subpoena was directed to records regarding the registrant, and not records regarding third party visitors to the website.

Several indictments issued during the months following the protests. In a superseding indictment dated on or about April 28, 2017, over 200 individuals were charged related to property damage and assault by individuals during the inauguration protests. The superseding indictment collectively defines the individuals charged as "Rioting Defendants," and describes the individuals who committed property damage and assault as a "Black Bloc."

B. The Search Warrant Dated July 12, 2017

DreamHost was served with the Search Warrant on July 17, 2017. See E-Mail dated July 18, 2017 from Karl Fry to Assistant United States Attorney John W. Borchert ("AUSA Borchert"), see Declaration of Karl Fry in Support of DreamHost Response ("Fry Decl.") Ex. A at 3. The

Search Warrant includes instructions for providing the warrant to DreamHost for "execution of a search." See D.C. Superior Court Search Warrant dated July 12, 2017, attached as Exhibit A to the United States' Motion for DreamHost to Show Cause ("Government Motion").[1] The Search Warrant states that probable cause exists for believing property "in violation of" the D.C. rioting statute will be found in "premises controlled by DreamHost, Inc. [sic]."[2] Id. The property is described as "stored electronic communications . . . as set forth more fully in Attachments A and B." Id.

Attachment A to the Search Warrant consists of a one-sentence description entitled "Property to Be Searched." See id., Attach. A. It describes the property as "information associated with www.disruptj20.org that is stored at" DreamHost. Id.

Attachment B to the Search Warrant is entitled "Particular Things to be Seized." Id., Attach. B at 1. The attachment identifies two categories of information: "Information to be disclosed by DreamHost" and "Information to be seized by the government." See id. (Emphasis added.) The first, "disclosure" category includes instructions that "DreamHost is required to disclose the [information listed] to the government for each account or identifier listed in Attachment A:." See id. The second, "seizure" category does not include any instructions. See id.

The "disclosure" category in Attachment B requires production of "all records or other information pertaining to [www.disruptj20.com], including all files, databases, and database records stored by DreamHost in relation to that account or identifier." Id. (Emphasis added.) Following this broad demand, the "disclosure" category includes three other descriptions of

[1] Unlike a traditional search warrant executed by government agents, the Search Warrant is more akin to a subpoena, as it requires DreamHost itself to execute the warrant and provide the responsive records to the government.

[2] Neither the remainder of the Search Warrant nor the government's brief explains how the electronic information sought is itself "in violation of" the D.C. statute, i.e., contraband, as opposed to evidence of a violation. DreamHost believes the use of this language in the Search Warrant is an error.

information sought: information identifying the subscribers and their payments; records pertaining to the types of service utilized by the user; and records pertaining to communications between DreamHost and anyone else regarding the account.

The "seizure" category in Attachment B consists of "all information described [in the 'disclosure' category] that constitutes fruits, evidence and instrumentalities of violations of D.C. Code § 22-1322 involving the individuals who participated, planed [sic], organized, or incited the January 20 riot, relating to the development, publishing, advertisement, access, use, administration or maintenance of [www.disruptj20.com] . . . ." Id.

Two different types of electronic data are listed as falling within the information subject to "seizure." See id. at 1-2. The first is "[f]iles, databases, and database records stored by DreamHost on behalf of the subscriber or user operating the website, including (a) programming code used to serve or process requests made via web browsers; (b) HTML, CSS, JavaScript, image files, or other files; (c) HTTP request and error logs; (d) SSH, FTP, or Telnet logs showing connections related to the website, and any other transactional information, including records of session times and durations, log files, dates and times of connecting, methods of connecting, and ports; (e) MySQL, PostgreSQL, or other databases related to the website; [and] (f) email accounts and the contents thereof, associated with the account." Id. The second is "[s]ubscriber information related to the accounts established to host [www.disruptj20.com]," including names and addresses, payment information, and domain registration details. Id. at 2.

C. DreamHost Attempts to Address Concerns with the Search Warrant

DreamHost's Compliance Team contacted AUSA Borchert on the evening of July 18, 2017 and informed AUSA Borchert that they were in receipt of the Search Warrant. See Karl Decl., Exhibit A at 3 submitted herewith. AUSA Borchert replied the next day, asking if DreamHost could produce the records that day. See id. at 2-3. Within a few hours, DreamHost's General

Counsel replied to AUSA Borchert and advised that all company personnel were offsite at an annual event and asked for additional time to respond. See id. at 5. The following day, Thursday, July 20, 2017, outside counsel for DreamHost contacted AUSA Borchert and advised that DreamHost was represented by counsel. See Exhibit A at 3 to the Declaration of Raymond O. Aghaian in Support of DreamHost's Response in Opposition to United States' Motion to Show Cause ("Aghaian Decl."). In the e-mail, DreamHost's counsel explained that DreamHost had questions relating to the search warrant, and asked to discuss the matter with AUSA Borchert on the afternoon of Friday, July 21, 2017, or Monday, July 24. See id. AUSA Borchert replied by voicemail on the same day, stating that he would like to discuss the matter the morning of Friday, July 21, 2017. See Aghaian Decl. ¶3. AUSA Borchert then followed this voicemail with an e-mail four minutes later asking Mr. Aghaian to instead contact him as soon as possible. See Aghaian Decl. Ex. A at 3.

Counsel for DreamHost replied to AUSA Borchert by e-mail that evening and advised that DreamHost would like to comply and produce the records, but that there were a few concerns DreamHost wanted to discuss. See id. at 2. Counsel for DreamHost offered to call AUSA Borchert at 11:30 a.m. PDT on Friday, July 21, 2017. See id. The following morning, AUSA Borchert responded that he might be in court at the proposed time, and inquired about DreamHost's concerns. See id. AUSA Borchert then left a voicemail for DreamHost's counsel at 10:01 a.m. PDT stating that DreamHost could send the government an email listing of any concerns. See Aghaian Decl. ¶4. AUSA Borchert then sent an e-mail four minutes later, asking if DreamHost could begin a "rolling production." See Aghaian Decl. Ex. A at 2. Counsel for DreamHost responded to AUSA Borchert in less than 45 minutes, advising that DreamHost wanted to resolve its concerns as expeditiously as possible so as to provide the records. See id. at

1-2. DreamHost's counsel listed the various concerns regarding the warrant, as instructed by AUSA Borchert. See id. Counsel offered to address the concerns with the government. See id.

AUSA Borchert did not respond. See Aghaian Decl. ¶5. Counsel for DreamHost followed up with the government again on Thursday, July 27. See Aghaian Decl. Ex. A at 1. Yet again, the government did not respond. See Aghaian Decl. ¶5. The government filed its motion to compel the next day.

D. The Website "disruptj20.org"

The website at issue is public and accessible to anyone over the internet. It appears to be a website for a political organization calling itself DisruptJ20 or #DisruptJ20, with the motto "#DisruptJ20 rejects all forms of domination and oppression, particularly those based on racism, poverty, gender & sexuality, organizes by consensus, and embraces a variety of tactics."[3] The website refers to "organizing," "resistance," "disruptions," and "civil disobedience," but does not describe acts of property damage or violence.

The website includes press releases from before the Inauguration ("Activists and organizers are planning massive protests and acts of resistance during the inauguration of Donald J. Trump on January 20") and after ("Our goals were: 1. Set a tone of resistance against the Trump administration; 2. Disrupt the normal flow of the inauguration; and 3. Empower local organizers in D.C. and give them skills and relationships to continue their work."). Press releases identified specific issues for protest at Inauguration checkpoints to include "racial justice, immigrant rights, LGBTQ+, antiwar, border justice, labor, climate, and other issues."

A portion of the website is dedicated to information concerning arrests on January 20. The website purports to offer a "legal guide" for J20 protestors, announcements of support for those arrested, and ways to contact the organization for further legal information, including by e-mail.

[3] #DISRUPTJ20 website, http://www.disuptj20.org (last visited July 31, 2017).

The website promotes several e-mail addresses using the disruptj20.org domain name and invites correspondence. Each of the accounts for the email addresses are assigned to a different user and each account contains a separate login password. See Fry Decl. at ¶3. The website also displays printable signs, mainly disparaging President Trump, and posts photographs of protesters with banners and signs and blogs regarding similar content.

III. Argument

A. The Search Warrant Violates the Fourth Amendment

1. Given the endangerment of First Amendment rights of third parties, the Search Warrant must be scrutinized with "particular exactitude."

In examining the features of the Search Warrant, the Court should begin with the way in which the warrant endangers the First Amendment interests of third parties, in this case the visitors to the website at issue. The Supreme Court has "recognized the vital relationship between freedom to associate and privacy in one's associations." NAACP v. Alabama ex rel. Patterson, 357 U.S. 449, 462 (1958). Where this constitutional protection "pertain[s] to political, economic, religious or cultural matters, and state action which may have the effect of curtailing the freedom to associate is subject to the closest scrutiny." Id. at 460-61.

The "[c]ompelled disclosure of membership in an organization engaged in advocacy of particular beliefs is of the same order. Inviolability of privacy in group association may in many circumstances be indispensable to preservation of freedom of association, particularly where a group espouses dissident beliefs." Id. at 462. Moreover, the Second Circuit Court of Appeals has noted: "[t]he Supreme Court has long recognized that an organization can assert associational privacy rights on behalf of its members, stating that '[i]t is hardly a novel perception that compelled disclosure of affiliation with groups engaged in advocacy may constitute ... a restraint

on freedom of association.'" Am. Civil Liberties Union v. Clapper, 785 F.3d 787, 802 (2d Cir. 2015) (citation omitted).[4]

Because it demands the disclosure to the government of "all files" related to the website, the Search Warrant requires DreamHost to produce the HTTP logs for visitors. HTTP logs contain extensive information about visitors to the website, including the time and date of the visit, the IP address for the visitor, the website pages viewed by the visitor (through their IP address), and even a detailed description of the software running in the visitor's computer. See Fry Decl. ¶4. This information, together with information from the internet service provider for the IP address, would allow the government to identify the specific computers used to visit the website, and what specifically was viewed on the website. See id. Pursuant to the government's preservation request, DreamHost has maintained HTTP logs for over 1,300,000 IP addresses of visitors to the website for a time frame after the rioting incidents. See id. ¶5.

In addition, DreamHost will be required to disclose all e-mails it maintains that are associated with the website, which will include e-mails sent in by third parties. See id. ¶6. DreamHost maintains membership lists for several e-mail discussion lists, from a number of different email accounts sponsored by the website. These discussion lists consist of groups of individual e-mail addresses. See id. ¶7. The Website promotes several e-mail addresses using the disruptj20.org domain name and invites correspondence. Each of the accounts for the email addresses are assigned to a different user and each account contains a separate login password. Id. ¶3.

Courts have specifically held that the government oversteps its authority when it seeks to obtain customer identities and records of activity in connection with protected speech, such as that

[4] One Court poignantly noted that "[c]oncerns about privacy are especially critical when people engage in aspects of speech and association during political campaigns, 'an area of the most fundamental First Amendment activities.'" State ex rel. Two Unnamed Petitioners v. Peterson, 363 Wis. 2d 1, 140 (2015) (citation omitted).

involved here. For instance, a demand for records relating to customer purchases from a website, requesting information on non-obscene purchases, was held to be overbroad. See In re Grand Jury Investigation of Possible Violation of 18 U.S.C. § 1461 et seq., 706 F. Supp. 2d 11, 21 (D.D.C. 2009). As the Court noted, the customers "enjoy a presumptive First Amendment right to receive [the materials] anonymously." Id. Similarly, even where the government's need to investigate was found to be legitimate in a federal tax evasion and wire fraud case of a used-book seller, the Court limited the records the government could obtain from on-line book-seller Amazon. See In re Grand Jury Subpoena to Amazon.com Dated Aug. 7, 2006, 246 F.R.D. 570, 572 (W.D. Wis. 2007). Similar to the Search Warrant here, Amazon was asked to produce the identities of the book buyers. Amazon filed a motion to quash the subpoena, leading the court to express serious First Amendment concerns about letting the government go through an individual's reading list. The compromise reached was to allow Amazon (not the government) to reach out and seek volunteer witnesses from the 24,000 purchasers. These individuals could then choose to contact the government and arrange an interview if they wanted, but "[a]nyone who wishes not to participate in this exercise, by virtue of his or her silence, will be left alone, and the government will never learn that person's identity or the titles of materials he/she purchased from D'Angelo through Amazon." Id. at 574.[5]

The disclosures of the information demanded by the Search Warrant will endanger the First Amendment interests of the innocent third parties who viewed or communicated with the website. It is not difficult to anticipate the impact this disclosure will have on the willingness of third parties

[5] See also In re Grand Jury Subpoena to Kramerbooks & Afterwords, Inc., where the government issued grand jury subpoenas to an independent bookstore and Barnes & Noble, seeking "all documents and things referring or relating to any purchase by Monica Lewinsky." The district court held that "the First Amendment is indeed implicated by the subpoenas," such that "the materials sought by the subpoenas would disclose specific titles of books purchased by Ms. Lewinsky, whose First Amendment rights are at issue here." The Court further held that the bookstores themselves were "also engaged in constitutionally protected expressive activities," namely, the circulation of books. Accordingly, the Court declined to enforce the subpoenas as issued, and ordered the Government to demonstrate both a compelling need for the materials it sought, and also explain why there was a sufficient connection between that information and the grand jury subpoenas. In re Grand Jury Subpoena to Kramerbooks & Afterwords, Inc., Nos. 98-135 (NHJ) and 98-138 (NHJ), 26 Med. L. Rptr. 1599, 1600 (D.D.C. April 6, 1998).

to investigate and engage with web sites of political organizations. United States Supreme Court cases "insist that the courts apply the warrant requirements with particular exactitude when First Amendment interests would be endangered by the search." Zurcher, 436 U.S. at 565 (emphasis added). This Court should not permit the government to trample upon the privacy of the individuals interacting with the website and force DreamHost to produce the electronic information that would not only identify who they are, but specifically what each of these individuals viewed, read or the political content that they were interested in.

2. Scrutinizing the Search Warrant with "particular exactitude" demonstrates that it violates the Fourth Amendment, both because it fails to describe the items to be seized with sufficient particularity and because the all-encompassing disclosures it requires are unreasonable.

Attachment B to the Search Warrant requires DreamHost to disclose to the government "all records or other information pertaining to" the website. The Search Warrant does not include any date restriction on this information. There is also no reference to any specific individual subject or target about whom information should be disclosed. Accordingly, any information (including information about visitors of the website), about any individual (multiple users here), regarding any and all email accounts (numerous email accounts here), at any time frame (even after the incident), are required to be disclosed by DreamHost.

From this practically unlimited set of electronic information concerning the website, the Search Warrant goes on to identify what is to be "seized." That is "all information" that "constitutes fruits, evidence and instrumentalities of violations of D.C. Code § 22-1322 involving the individuals who participated, planed [sic], organized, or incited the January 20 riot, relating to the development, publishing, advertisement, access, use, administration or maintenance of" the website. The Search Warrant mentions, as a category of information to be seized, "files, databases, and database records stored by DreamHost on behalf of the subscriber or user operating the website." Examples of these files are "HTTP request logs," which, as discussed above, contain

extensive information about visitors to the website, and "email accounts and the contents thereof associated with the account." As with the information to be disclosed, there is no date restriction on the information to be seized.

The Search Warrant will result in the disclosure of large quantities of information, including information about third parties. For example, during six days after the Inauguration, the website received over 1,300,000 HTTP requests, each which generated an IP log of the visit. See Fry Decl. ¶5. DreamHost also maintains over 2,000 images related to the website. See id. ¶8. Despite this volume of data, the Search Warrant does not describe any protocol for searching it. Nor does the Search Warrant explain what will happen to the information the government obtains that is not subject to "seizure" because it is not evidence of a crime.

The Search Warrant's "two-step" approach to obtaining electronic information – where the government gets a vast set of data without probable cause to that set, and then "seizes" a sub-set of the data with probable cause – is not without controversy. A number of courts have found the approach flawed under the Fourth Amendment. See In re Search of Info. Associated with [redacted]@mac.com that is Stored at Premises Controlled by Apple, Inc., 25 F. Supp. 3d 1, 6-7 (D. D.C. 2014), vacated, 13 F. Supp. 3d 157 (D. D.C. 2014) ("Apple") (rejecting the "two-step" procedure for obtaining complete e-mail accounts); In re: [Redacted]@gmail.com, 62 F. Supp. 3d 1100, 1105 (N.D. Cal. 2014) (denying search warrant application after finding "two-step" procedure unreasonable under the Fourth Amendment); In re Search of Premises Known as Three Hotmail Email Accounts, 2016 WL 1239916, *13 (D. Kan. 2016), overruled in part sub nom. In re Search of Info. Associated with Email Addresses Stored at Premises Controlled by Microsoft Corp., 212 F. Supp. 3d 1023 (D. Kan. 2016) ("Microsoft") (denying search warrant application for e-mail accounts, comparing the warrant to one "asking the post office to provide copies of all mail ever sent by or delivered to a certain address so that the government can open and read all the mail

to find out whether it constitutes fruits, evidence or instrumentality of a crime"); In re Search of Info. Associated with the Facebook Account Identified by the Username Aaron.Alexis that is Stored at Premises Controlled by Facebook, Inc., 21 F. Supp. 3d 1, 7 (D.D.C. 2013) ("Facebook") (imposing minimization procedures where search warrant requested by government for Facebook account "unduly invaded the privacy of third parties" by requesting records of communications between third parties and a Facebook account); In re Search of Info. Associated with 15 Email Addresses Stored at Premises Owned, Maintained, Controlled or Operated by 1&1 Media, Inc., Google, Microsoft, and Yahoo!, Case No. 2:17-cm-03152 (M.D. Ala. July 14, 2017) ("1&1 Media") (denying search warrant application for e-mail accounts as requesting permission for "a general, exploratory rummaging") (attached as Exhibit B to Aghaian Decl.). Similarly, the Search Warrant invites this controversy by seeking the disclosure of every "record or other information" pertaining to www.disruptj20.org, including associated e-mail, without probable cause for this practically unlimited scope of information concerning the website.

Moreover, every search warrant must satisfy the particularity requirement of the Fourth Amendment, including that the "things to be seized" are described with specificity. See Dalia v. United States, 441 U.S. 238, 255 (1979). "The manifest purpose of th[e] particularity requirement was to prevent general searches." Maryland v. Garrison, 480 U.S. 79, 84 (1987). These were searches "abhorred by the colonists . . . a general, exploratory rummaging in a person's belongings." Coolidge v. New Hampshire, 403 U.S. 443, 467 (1971).

The Search Warrant's description of the things to be seized does not pass the particularity test. It defines what is to be seized in three ways. First, it is information that "constitutes fruits, evidence, and instrumentalities of violations of" the rioting statute "involving the individuals who participated, planed [sic], organized, or incited the January 20 riot." Second, the information "relat[es] to the development, publishing, advertisement, access, use, administration or

maintenance of" the website. Third, the information to be seized includes "files, databases, and database records." Yet, describing the information to be seized as evidence of a crime "involving" unnamed participants in the crime does not provide any meaningful specificity. Compare Apple, 13 F. Supp. 3d at 161 (description of things to be seized identified the information as "involving any or all of the following: [individuals and entities . . .]"). Limiting the information seized to that "relating to" the "publishing" or "use" of the website also lacks the required specificity, since practically any conceivable information about a web site is related to its publishing or use. Similarly, even if the use of the term "including" after the preceding broad description imposed some limit on the information to be seized, which it does not, limiting the seizure to electronic "files, databases, and database records" is no limit at all. Finally, the lack of a date range alone fails the specificity test. See Microsoft, 212 F. Supp. 3d at 1036 ("In cases in which courts have either denied a search warrant for the entirety of an email account or suppressed evidence based on an overbroad search warrant, the warrants lacked particularity, for example, in identifying a specified date range . . . .").

The combination of the broad disclosure required by the Search Warrant implicating First Amendment issues and the lack of specificity in its description of the information to be seized implicates the Fourth Amendment's reasonableness requirement. This is of particular significance where the Government is asking a private entity to determine what is responsive to a search warrant without such specificity. "As the text of the Fourth Amendment indicates, the ultimate measure of the constitutionality of a governmental search is reasonableness." Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646, 652 (1995) (internal quotation marks omitted); see also In re G.B., 139 A.3d 885, 897 (D.C. 2016). "[W]here the legality of the Government's conduct already depends upon an attenuated construction of what constitutes a seizure, the court should be particularly scrupulous in holding the Government to its burden to show that its conduct is reasonable." 1 & 1

Media, Aghaian Decl. Ex. B, at 7-8. Because the Search Warrant allows the government to obtain large amounts of information, including the content of e-mail communications, initiated by innocent third parties, fails to identify with sufficient specificity what will be seized, and does not explain to DreamHost what will happen to the large quantities of un-seized information, the Search Warrant is not reasonable under the Fourth Amendment. See Facebook, 21 F. Supp. 3d at 7 (imposing Fourth Amendment minimization procedures where government "will have to see third party communications that are innocuous and irrelevant and sent by persons who could not possibly have anticipated that the government would see what they have posted").

B. The Search Warrant Violates the Privacy Protection Act

The Privacy Protection Act ("PPA") makes it unlawful for a government officer, in connection with the investigation or prosecution of a criminal offense, to search for or seize "work product" or "documentary materials" that are possessed by a person "in connection with a purpose to disseminate to the public a newspaper, book, broadcast, or other similar form of public communication." 42 U.S.C. §§ 2000aa (a), (b) (1996).

The PPA provides "First Amendment Privacy Protection" and was passed in response to the Supreme Court's much shunned Zurcher decision. See generally, 436 U.S. 547 (1970); see text accompanying note 6. In Zurcher, the Supreme Court had ruled that the execution of a search warrant at the offices of a university newspaper did not violate the Fourth Amendment. Much like here, the search occurred following a demonstration at Stanford University Hospital in which policemen had been injured. After the demonstration, the paper had published "articles and photographs devoted to the hospital protest and the violent clash between demonstrators and police." Id. at 551.[6] PPA protections are not limited to the traditional press and also protect

[6] "The very purpose of the Privacy Protection Act is to protect materials that document matters of public interest. After all, the Act was passed in response to Zurcher v. Stanford Daily, 436 U.S. 547, 98 S.Ct. 1970, 56 L.Ed.2d 525 (1978), in which the Supreme Court upheld the search of a newspaper office for materials depicting a violent clash

"academicians, authors, filmmakers, and free lance [sic] writers and photographers." H.R. Rep. No. 96-1064, at 5 (1980).

Under the PPA, "documentary materials" are defined as "materials upon which information is recorded." 42 U.S.C. § 2000aa-7(a). Documentary materials include: "written or printed materials, photographs . . . and other mechanically, magnetically [sic] or electronically recorded cards, tapes or discs." Id. Moreover, "work product" includes materials created "in anticipation of communicating such materials to the public," and such material can include "mental impressions, conclusions, opinions, or theories." Id. §2000aa-7(b). Excluded from the definition for either "documentary materials" or "work product" are "property designed or intended for use, or which is or has been used, as the means of committing a criminal offense." Id. §§ 2000aa-7(a), (b).

The legislative history to the PPA provides: ". . . the Committee recognized a problem for the law enforcement officer, who seeking to comply with the statute, might be uncertain whether the materials he sought were work product or nonwork product and that they were intended for publication. Therefore, in the interests of allowing for some objective measure for judgment by the office, the Committee has provided that the work product must be possessed by someone "reasonably believed" to have a purpose to communicate to the public." S.Rep. No. 96-874, at 10 (1980), reprinted in 1980 U.S.C.C.A.N. 3950, 3957."

As the provider of a web hosting service, DreamHost hosts the www.disruptj20.org website and all of the corresponding data. The website disseminates the data it publishes through DreamHost, to include press releases, messages, photographs, and other images, to the public. See Fry Decl. ¶9. *See* Steve Jackson Games, Inc. v. United States Secret Service, 816 F. Supp. 432, 440 (W.D. Tex. 1993), aff'd 36 F.3d 457 (5th Cir. 1994) (noting information related to a public electronic bulletin board constituted "documentary materials" under the PPA). The

---

between demonstrators and police at a university hospital—that is, a highly public event." Binion v. City of St. Paul, 788 F. Supp. 2d 935, 948 (D. Minn. 2011)

"disruptj20.org" website, through DreamHost, was publishing and disseminating information and images to the public. Much of the information in possession of DreamHost was published to the public through "disruptj20.org." Fry Decl. ¶10. Yet, other material, to include numerous draft blog posts, hundreds of images, including metadata for the images via detailed "datafields" that include titles and explanations for the images, do not appear to have been previously published. See id. The unpublished materials appear to be similar to the material that were previously published. It is difficult to determine if the apparent unpublished materials are preserved for a future publication date, such as an Inauguration Day anniversary event, or if the creator of the material previously excluded such material from publication. See Fry Decl. ¶11. Moreover, just as the time frame relating to the information about visitors to the website is after the rioting incident date, some of the apparent unpublished material referenced above appears to be created after the day of the rioting incident as well. See id.

Based on DreamHost's review of the data, much of this material appears that it could qualify either as "work product," "documentary material," or both. Without any specification from the government, particularly given the over-expansive language of the Search Warrant, the Court should not compel DreamHost to provide all material to the government without a determination whether such material is intended for publication and if such material qualifies either as "work product" or "documentary material."

In its motion, the government argues that the PPA provides only one "exclusive" remedy for a violation – a civil cause of action for damages. Government Motion at 6. However, a review of the section cited by the government shows that this remedy is only exclusive of "any other civil action or proceeding . . . against the officer or employee whose violation gave rise to the claim, or against the estate of such officer or employee." 42 U.S.C. §2000aa-6(d). The statute does not bar

DreamHost from raising the Act in a challenge to the Search Warrant itself, the very process at the center of the statute's protections.

C. D.C. Law Does Not Authorize Extraterritorial Search Warrants

The Search Warrant is extraterritorial, i.e., issued from the District of Columbia but directed at electronic data stored in Oregon. However, D.C. law only provides for search warrants executed "in the District of Columbia." D.C. Code §23-521(a) (2011). To resolve this conflict, the government takes the position that the Search Warrant is authorized by the federal Stored Communications Act, 18 U.S.C. §§ 2701 et seq. See Government's Motion at p. 5.

The Search Warrant generally falls within the SCA because it seeks the contents of communications in electronic storage from DreamHost, a provider of electronic communication service. See 18 U.S.C. § 2703(a). The SCA requires a warrant for this information if it has been in storage for 180 days or less, or longer if no notice is given to the customer. See id. The SCA requires that the warrant be "issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction." Id. The SCA defines the term "court of competent jurisdiction" to include (1) any federal court with (a) jurisdiction over the offense being investigated or (b) in a district in which the service provider is located or information is stored; and (2) "a court of general criminal jurisdiction of a State authorized by the law of that State to issue search warrants." 18 U.S.C. § 2711(3). The term "State" includes the District of Columbia. See 18 U.S.C. §§ 2510(3) & 2711(1).

The government argues that the above definition of what constitutes a "court of competent jurisdiction" empowered the D.C. Superior Court to issue the Search Warrant for execution outside of the District of Columbia. The government cites no authority for this interpretation, however. Indeed, the government's contention about the effect of this language is flatly contradicted by the

courts that have considered the issue. See State v. Rose, 330 P.3d 680, 685 (Or. Ct. App. 2014) ("The SCA does not expressly address whether a state court can issue a search warrant for such content located in another state."); In re Search Warrant for Records from AT&T, 2017 WL 2511269, at *3 (N.H. June 9, 2017) (same, quoting Rose).

Instead, both the Oregon and New Hampshire courts looked to state law to answer the question of whether extraterritorial state search warrants were permitted. In Rose, the Oregon Court of Appeals relied on an Oregon statute that authorized Oregon courts to issue warrants "regardless of whether the recipient or the papers, documents, records or things are located within this state." Rose, 330 P.3d at 685. In the AT&T case, the New Hampshire Supreme Court explained that New Hampshire law "does not expressly limit the [trial court's] authority to issue search warrants based upon the location of the property or article sought." AT&T, 2017 WL 2511269, at *3. Relying on their analyses of state law, both courts concluded that the extraterritorial search warrants were permitted.[7]

In contrast, the District of Columbia lacks a law that authorizes extraterritorial search warrants. Nor, unlike New Hampshire law, is D.C. law silent on the issue – D.C. Code §23-521(a) provides that a warrant may authorize a search "in the District of Columbia" only. Looking at D.C. law, as required, the extraterritorial Search Warrant is unauthorized and invalid.

IV. Conclusion

[7] In Hubbard v. MySpace, Inc., 788 F. Supp. 2d 319 (S.D.N.Y. 2011), a federal district court concluded that an extraterritorial search warrant issued by a Georgia state magistrate judge was valid because federal magistrates had the ability to issue such search warrants and a Georgia statute incorporated federal law on the subject. Here, by contrast, there is no equivalent D.C. law. Furthermore, Hubbard addressed a prior version of the SCA. The current version of the SCA treats federal and state jurisdiction differently, by specifically defining only the federal "court of competent jurisdiction" in jurisdictional terms -- as "any [federal] district court . . . that . . .has jurisdiction over the offense being investigated [.]" 18 U.S.C. § 2711(3)(A)(i); Rose, 330 P.3d at 685 n.5 ("[U]nder the SCA, a federal court in Oregon could issue a warrant compelling the disclosure of content in another state so long as the court has territorial jurisdiction over the offense related to the warrant.").

Because it requires the disclosure of every piece of electronic information related to a website, including a large amount of information about the protected activities of third parties, the government's Search Warrant requires scrutiny of "particular exactitude." Scrutiny of this type demonstrates that the warrant lacks the specificity required by the Fourth Amendment and is unreasonable as a whole. In addition, the Search Warrant violates the Privacy Protection Act and was not authorized by District of Columbia law. For the foregoing reasons, DreamHost respectfully requests that the government's motion be denied.

Dated this 11th day of August, 2017.

By: /s/ Raymond O. Aghaian
Raymond O. Aghaian
D.C. Bar #478838
Kilpatrick Townsend & Stockton LLP
9720 Wilshire Blvd PH
Beverly Hills, CA 90212-2018
raghaian@kilpatricktownsend.com
(310) 310-7010 office
(310) 388-1198 facsimile
Attorney for DreamHost, LLC

Chris Ghazarian, Esq. (*Pro Hac Vice to be submitted)*
DreamHost, LLC
707 Wilshire Blvd., Suite 5050
Los Angeles, CA 90017
chris@dreamhost.com
(213) 787-4401 office
Attorney for DreamHost, LLC

CERTIFICATE OF SERVICE

A true and correct copy of the foregoing was sent via e-mail and CaseFileXpress this 11th day of August, 2017, to:

AUSA John W. Borchert
U.S. Attorney's Office
555 Fourth Street, N.W.
Washington, D.C. 20530
john.borchert@usdoj.gov

/s/ Raymond O. Aghaian
Raymond O. Aghaian

SUPERIOR COURT OF THE DISTRICT OF COLUMBIA

CRIMINAL DIVISION – FELONY BRANCH

In the Matter of the Search of www.disruptj20.org that Is Stored at Premises Owned, Maintained, Controlled, or Operated by DreamHost	**)**	**Special Proceeding No. 17 CSW 3438**
	)	**Judge Leibovitz**
	)	**Hearing: 9:30 a.m. Friday, Aug. 18, 2017**

DECLARATION OF RAYMOND O. AGHAIAN IN SUPPORT OF DREAMHOST'S RESPONSE IN OPPOSITION TO UNITED STATES' MOTION TO SHOW CAUSE

I, RAYMOND O. AGHAIAN, declare, under penalty of perjury as follows:

1. I am a partner with the law firm Kilpatrick Townsend & Stockton LLP, counsel to DreamHost, LLC ("DreamHost").

2. Attached as Exhibit A is a true and correct copy of e-mails exchanged between the government and DreamHost and its counsel during the time period of July 14, 2017 through July 27, 2017.

3. On Thursday, July 20, 2017, I received a voicemail from Assistant United States Attorney John W. Borchert. In the voicemail, AUSA Borchert stated that he would like to discuss the search warrant that had been issued to DreamHost the following morning, Friday, July 21, 2017.

4. On Friday, July 21, 2017, at 10:01 a.m. PDT, I received a second voicemail from AUSA Borchert. In the voicemail, AUSA Borchert informed me that DreamHost could submit to the government a list of any concerns regarding the search warrant.

5. AUSA Borchert did not respond to the e-mail I sent him on July 21, 2017, which listed concerns with the search warrant. Nor did AUSA Borchert respond to the follow-up e-mail I sent him on July 27, 2017.

6. Attached as Exhibit B is a true and correct copy of the July 14, 2017 Order in In the Matter of the Search of Information Associated with Fifteen Email Addresses Stored at Premises Owned, Maintained, Controlled or Operated by 1 & 1 Media, Inc., Google, Inc., Microsoft Corp., and Yahoo! Inc., Case No. 2:17-cm-03152-WKW-WC (N.D. Ala.).

I declare under penalty of perjury under the laws of the State of California that the foregoing is true and correct, and that this Declaration is executed on August 11, 2017 in Beverly Hills, California

/s/Raymond O. Aghaian
Raymond O. Aghaian

CERTIFICATE OF SERVICE

A true and correct copy of the foregoing was sent via e-mail and CaseFileXpress this 11th day of August, 2017, to:

AUSA John W. Borchert
U.S. Attorney's Office
555 Fourth Street, N.W.
Washington, D.C. 20530
john.borchert@usdoj.gov

/s/ Raymond O. Aghaian
Raymond O. Aghaian

From: Aghaian, Raymond
Sent: Thursday, July 27, 2017 1:15 PM
To: Borchert, John (USADC)
Cc: Kerkhoff, Jennifer (USADC)
Subject: RE: Search Warrant and Preservation (LGL-74338)

Hi John,

Just following up on the below to see how you would like to proceed on the search warrant. Thanks.

Ray

Raymond O. Aghaian
Kilpatrick Townsend & Stockton LLP
9720 Wilshire Blvd PH | Beverly Hills, CA 90212-2018
office 310 310 7010 | fax 310 388 1198 raghaian@kilpatricktownsend.com | www.kilpatricktownsend.com

-----Original Message-----
From: Aghaian, Raymond
Sent: Friday, July 21, 2017 10:43 AM
To: 'Borchert, John (USADC)'
Cc: Kerkhoff, Jennifer (USADC)
Subject: RE: Search Warrant and Preservation (LGL-74338)

John,

Sorry I missed your call this morning, busy morning. There are a few concerns and we would like to resolve as expeditiously as possible to get you the production. My concerns consist of the following:

1. There is some uncertainty as to the language in Section II, paragraph 2, that we would like to clarify and get a better understanding of what exactly is requested. Moreover, we need to be able to inform the subscriber about the warrant, but it is difficult to do so without knowing specifically which accounts or domains are at issue.

2. The DC Code is very specific about the Superior Court's jurisdictional limit in issuance of search warrants within DC. Since the servers containing the records at issue here are located in Portland, Oregon, instead of DC, we would like to ask that you seek the warrants from the appropriate court.

3. Some of the requested information likely falls under the protected category of information under the Privacy Protection Act and is not subject to search and seizure pursuant to a search warrant;

4. Some of the information requested appears overbroad, requesting what amounts to all data without any limitations or a specified timeframe, likely constituting an overseizure. For instance, in one of the requests, the warrant seeks the IP addresses of over 1,000,000 visitors to the website.

My suggestion would be to resolve concerns 1 and 2 first and then allow DreamHost to begin expeditiously making the rolling production to either the Court or a special master for the records at issue so we can resolve the concerns before

making the production to the government. Please let me know your thoughts and we can proceed accordingly. Thank you.

Ray

Raymond O. Aghaian
Kilpatrick Townsend & Stockton LLP
9720 Wilshire Blvd PH | Beverly Hills, CA 90212-2018
office 310 310 7010 | fax 310 388 1198 raghaian@kilpatricktownsend.com | www.kilpatricktownsend.com

-----Original Message-----
From: Borchert, John (USADC) [mailto:John.Borchert@usdoj.gov]
Sent: Friday, July 21, 2017 10:04 AM
To: Aghaian, Raymond
Cc: Kerkhoff, Jennifer (USADC)
Subject: RE: Search Warrant and Preservation (LGL-74338)

Hello, Ray - I just tried again to reach you on the phone and left another message. Can a rolling production start today?

Regards,

John

-----Original Message-----
From: Borchert, John (USADC)
Sent: Friday, July 21, 2017 6:59 AM
To: Aghaian, Raymond <RAghaian@kilpatricktownsend.com>
Cc: Kerkhoff, Jennifer (USADC) <JKerkhoff@usa.doj.gov>
Subject: Re: Search Warrant and Preservation (LGL-74338)

Great. I'm not certain I'll be out of court at that time. What are the concerns? A rolling production of whatever they have ready now is fine.

Sent from my iPhone

> On Jul 21, 2017, at 1:37 AM, Aghaian, Raymond <RAghaian@kilpatricktownsend.com> wrote:
>
> John - Thanks for the response. They would like to comply and produce, but I have a few concerns I would like discuss. I can call you at 11:30 a.m. PST, if you are available then. Thanks.
>
> Ray
>
> Raymond O. Aghaian
> Kilpatrick Townsend & Stockton LLP
> 9720 Wilshire Blvd PH | Beverly Hills, CA 90212-2018
> office 310 310 7010 | fax 310 388 1198 raghaian@kilpatricktownsend.com
> | www.kilpatricktownsend.com
>
>
>

> -----Original Message-----
> From: Borchert, John (USADC) [mailto:John.Borchert@usdoj.gov]
> Sent: Thursday, July 20, 2017 4:57 PM
> To: Aghaian, Raymond
> Cc: Kerkhoff, Jennifer (USADC)
> Subject: Re: Search Warrant and Preservation (LGL-74338)
>
> Hello, Ray-
>
> I just tried to reach you. Please call me as soon as possible at either of my numbers below. If your client is unwilling to begin an immediate rolling production, I will need to seek relief from the Court.
>
> Regards,
>
> John
>
>
> Sent from my iPhone
>
> On Jul 20, 2017, at 6:22 PM, Aghaian, Raymond
<RAghaian@kilpatricktownsend.com<mailto:RAghaian@kilpatricktownsend.com>> wrote:
>
> Hi John,
>
> I represent DreamHost and I have just been retained in the above referenced matter. I have a number questions regarding the search warrant that I would like to discuss with you. Can you please let me know your availability to discuss for either tomorrow afternoon or sometime on Monday? Thank you.
>
> Ray
>
> Raymond O. Aghaian
> Kilpatrick Townsend & Stockton LLP
> 9720 Wilshire Blvd PH | Beverly Hills, CA 90212-2018 office 310 310
> 7010 | fax 310 388 1198
> raghaian@kilpatricktownsend.com<mailto:raghaian@kilpatricktownsend.com
> > | My
> Profile<http://www.kilpatricktownsend.com/en/Who%20We%20Are/Profession
> als/A/AghaianRaymondO16681.aspx> |
> vCard<http://www.kilpatricktownsend.com/_assets/vcards/professionals/A
> ghaianRaymondO.vcf>
>
>
> From: "Borchert, John (USADC)"
> <John.Borchert@usdoj.gov<mailto:John.Borchert@usdoj.gov>>
> Date: Jul 20, 2017 4:05 AM
> Subject: RE: Search Warrant and Preservation (LGL-74338)
> To: "Christopher Ghazarian"
> <christopher.ghazarian@dreamhost.com<mailto:christopher.ghazarian@drea
> mhost.com>>
> Cc: "legal@dreamhost.com<mailto:legal@dreamhost.com>"
> <legal@dreamhost.com<mailto:legal@dreamhost.com>>, "Kerkhoff, Jennifer
> (USADC)"

> <Jennifer.Kerkhoff@usdoj.gov<mailto:Jennifer.Kerkhoff@usdoj.gov>>
>
> Thanks, Chris. Please go ahead and begin a "rolling" production of what you have ready now. I would expect you have some materials that you could produce today, but let me know if I have that wrong.
>
> Regards,
>
> John
>
> From: Christopher Ghazarian
> [mailto:christopher.ghazarian@dreamhost.com<mailto:christopher.ghazari
> an@dreamhost.com>]
> Sent: Wednesday, July 19, 2017 1:57 PM
> To: Borchert, John (USADC)
> <JBorchert@usa.doj.gov<mailto:JBorchert@usa.doj.gov>>
> Cc: legal@dreamhost.com<mailto:legal@dreamhost.com>; Kerkhoff,
> Jennifer (USADC) <JKerkhoff@usa.doj.gov<mailto:JKerkhoff@usa.doj.gov>>
> Subject: Re: Search Warrant and Preservation (LGL-74338)
>
> Hi John,
>
> DreamHost is having its annual "All Hands" meeting; the entire company gathers offsite for a day-long meeting, and we're all out of the office in order to attend.
>
> You asked Karl about producing the data immediately since it has been "preserved since January." After reviewing the warrant, it looks like you are requesting additional data that wasn't included in the preservations ("any messages, records, files, logs, or information that have been deleted but are still available to DreamHost...."). Thus, in order for us to comply with your warrant, Karl is pulling all of the new information from our database.
>
> We kindly request additional time to put together what you're asking for once we're back in the office, and we will have an update for you as soon as possible (likely tomorrow) with production information and instructions.
>
>
> Best,
>
> Chris Ghazarian | General Counsel
> 213.787.4401<tel:(213)%20787-4401> |
> chris@dreamhost.com<mailto:chris@dreamhost.com> |
> chris.law<https://www.linkedin.com/in/christopher-ghazarian-6917a528>
> 707 Wilshire Blvd, Suite 5050, Los Angeles, CA 90017
>
> <image001.png>
>
>
>
>
> On Jul 19, 2017, at 6:04 AM, Borchert, John (USADC) <John.Borchert@usdoj.gov<mailto:John.Borchert@usdoj.gov>> wrote:
>
> Hello, Karl -
>

> Thanks for your response. I sent a courtesy copy of the warrant to you last week, and you've had the data preserved since January. Can you please provide the materials to us today? If not, we may need to seek relief from the Court.
>
> Regards,
>
> John
>
> From: Karl Fry [mailto:karl.fry@dreamhost.com]
> Sent: Tuesday, July 18, 2017 8:31 PM
> To: Borchert, John (USADC)
> <JBorchert@usa.doj.gov<mailto:JBorchert@usa.doj.gov>>;
> legal@dreamhost.com<mailto:legal@dreamhost.com>
> Cc: Kerkhoff, Jennifer (USADC)
> <JKerkhoff@usa.doj.gov<mailto:JKerkhoff@usa.doj.gov>>
> Subject: Re: Search Warrant and Preservation (LGL-74338)
>
> Hi John,
>
> We are in receipt of the warrant that was served yesterday; thank you. We have quite a bit going on this week, but I will be in touch as soon as I have more information for you.
> We do appreciate your patience in the meantime.
> Sincerely,
> Karl Fry
> DreamHost Compliance Team
> http://www.dreamhost.com<http://www.dreamhost.com/>
>
> On 7/18/17 10:45 AM, Borchert, John (USADC) wrote:
> Hello, Karl -
>
> You were personally served by the FBI yesterday. Can you please make a production to us today?
>
> Regards,
>
> John
>
> John W. Borchert
> Deputy Chief -- Felony Major Crimes Trial Section Misdemeanor Trial
> Unit U.S. Attorney's Office for the District of Columbia
> Desk: 202-252-7679<tel:(202)%20252-7679> Mobile:
> 202-870-6071<tel:(202)%20870-6071>
> john.borchert@usdoj.gov<mailto:john.borchert@usdoj.gov>
>
>
> From: Karl Fry [mailto:karl.fry@dreamhost.com]
> Sent: Friday, July 14, 2017 7:56 PM
> To: Borchert, John (USADC)
> <JBorchert@usa.doj.gov><mailto:JBorchert@usa.doj.gov>;
> legal@dreamhost.com<mailto:legal@dreamhost.com>
> Subject: Re: Search Warrant and Preservation (LGL-74338)
>
> Hi John,
>

> Just as a reminder -- DreamHost does not accept substituted service for production orders. We respectfully request that such orders be served either in person at our downtown Los Angeles location, or with our registered service agent CT Corporation. The addresses for both can be found on our website, here:
>
> https://www.dreamhost.com/legal/government-requests/
>
> If you already intend to serve in person as well, please disregard.
>
> Thanks,
> Karl Fry
> DreamHost Compliance Team
> http://www.dreamhost.com<http://www.dreamhost.com/>
>
>
> On 7/14/17 1:49 PM, Borchert, John (USADC) wrote:
> Hello, Karl -
>
> I have attached a search warrant that we have obtained for the disruptj20 website. Our preservation for this account dates back to January 17. I am also attaching an additional preservation letter dated today. Please let me know if you have any questions.
>
> Regards,
>
> John
>
> John W. Borchert
> Deputy Chief -- Felony Major Crimes Trial Section Misdemeanor Trial
> Unit U.S. Attorney's Office for the District of Columbia
> Desk: 202-252-7679<tel:(202)%20252-7679> Mobile:
> 202-870-6071<tel:(202)%20870-6071>
> john.borchert@usdoj.gov<mailto:john.borchert@usdoj.gov>
>
>
>
>
>
> _____
>
> Confidentiality Notice:
> This communication constitutes an electronic communication within the meaning of the Electronic Communications Privacy Act, 18 U.S.C. Section 2510, and its disclosure is strictly limited to the recipient intended by the sender of this message. This transmission, and any attachments, may contain confidential attorney-client privileged information and attorney work product. If you are not the intended recipient, any disclosure, copying, distribution or use of any of the information contained in or attached to this transmission is STRICTLY PROHIBITED. Please contact us immediately by return e-mail or at 404 815 6500, and destroy the original transmission and its attachments without reading or saving in any manner.
>
> _____
>
> ***DISCLAIMER*** Per Treasury Department Circular 230: Any U.S. federal tax advice contained in this communication (including any attachments) is not intended or written to be used, and cannot be used, for the purpose

of (i) avoiding penalties under the Internal Revenue Code or (ii) promoting, marketing or recommending to another party any transaction or matter addressed herein.

IN THE DISTRICT COURT OF THE UNITED STATES
FOR THE MIDDLE DISTRICT OF ALABAMA
NORTHERN DIVISION

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH FIFTEEN EMAIL ADDRESSES STORED AT PREMISES OWNED, MAINTAINED, CONTROLLED OR OPERATED BY 1 & 1 MEDIA, INC., GOOGLE, INC., MICROSOFT CORP., and YAHOO! INC.	)	Case No. 2:17CM3152-WC

ORDER

On June 15, 2017, the United States presented fifteen separate applications for search warrants related to its investigation of alleged identity theft and related fraudulent tax filings.[1] After careful review of the applications, the undersigned Magistrate Judge concludes that, for the reasons given below, the applications are due to be denied.

I. THE APPLICATIONS

In each of the fifteen applications for search warrants, the United States seeks permission to require the above-captioned electronic communications service providers ("ECSP"s) to provide the United States with information associated with a particular email account stored, maintained, controlled, or operated by the provider. The applications are based largely upon the same asserted probable cause, with variations pertaining to specific communications to and from the email account that is the subject of that specific warrant application. As presented to the undersigned, the warrant applications are structured as

[1] Because the Government requested that the warrant applications be filed under seal, they are attached as sealed exhibits to this Order.

follows: Attachment A to the search warrant describes the thing or property to be searched—i.e., the email account and the ECSP that owns, maintains, controls, or operates the email account—and Attachment B defines, in two separate parts, the "Particular Items to be Seized." Part One of Attachment B describes the information that the warrant requires the ECSP to provide to the Government, including the following:

> a. The contents of all e-mails associated with the account, including stored or preserved copies of e-mails sent to and from the account, draft e-mails, the source and destination addresses associated with each e-mail, the date and time at which each e-mail was sent, and the size and length of each e-mail;
>
> b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated session times and dates, account status, alternative e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);
>
> c. The types of service utilized;
>
> d. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files;
>
> e. All records pertaining to communications between [the ECSP] and any person regarding the account, including contacts with support services and records of actions taken.
>
> f. All location data associated with the account.
>
> g. All location history associated with the account, whether derived from Global Positioning System (GPS) data, cell site/cell tower triangulation/trilateration, and precision measurement information such as timing advance or per call measurement data, and Wi-Fi location. Such data

shall include the GPS coordinates and the dates and times of all location recordings.

h. All identity and contact information, including full name, e-mail address, physical address (including city, state, and zip code), date of birth, phone numbers, gender, hometown, occupation, and other personal identifiers.

Part Two of Attachment B describes the "information to be seized by the Government" as follows:

All information described above in Section 1 that constitutes fruits, evidence and instrumentalities of violations of Title 18, United States Code, Section 1028A; Title 18, United States Code, Section 1030; and title 18, United States Code, Section 1343 since January 1, 2015, including information pertaining to:

a. Records and communications regarding the transmission of personally identifiable information, IRS Forms W-2, tax returns, prepaid debit cards, the proceeds of the transfer or use of personally identifiable information, and a conspiracy to file false tax returns using stolen identities;

b. Records and communications regarding any property derived from the proceeds of the conspiracy;

c. Records relating to who created, used, or communicated with the account or identifier, including records about their identities and whereabouts; and

d. Records indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner, including all geolocation information.

e. Records relating to the identities of the person(s) who communicated with the user ID about matters described in paragraph 2.a., including records that help reveal their whereabouts.

In addition to describing the probable cause underlying the Government's requests, the

affidavits in support of the search warrant provide a cursory description of the Government's planned search methodology. The affiant swears that he will use the warrant to require the ECSP "to disclose to the government copies of the records and other information (including the content of communications) particularly described in Attachment A and Section 1 of Attachment B. Upon receipt of the information described in Section 1 of Attachment B, government-authorized persons will review that information to locate the items described in Section 2 of Attachment B."

II. DISCUSSION

For the sake of brevity and convenience to the court and the Government, and to facilitate the prompt anticipated appeal of this Order, the undersigned will forego a rigorous discussion of the Fourth Amendment principles undergirding the undersigned's concern with the Government's search warrant requests. It is sufficed for present purposes to note, and the undersigned does not believe that the Government would disagree, "that indiscriminate searches and seizures conducted under the authority of 'general warrants' were the immediate evils that motivated the framing and adoption of the Fourth Amendment[,]" *Payton v. New York*, 445 U.S. 573, 583 (1980); that the Fourth Amendment's particularity requirement is the primary means by which the Constitution seeks to guard against such "indiscriminate searches and seizures," *Coolidge v. New Hampshire*, 403 U.S. 443, 467 (1971); that Fourth Amendment protections—including the prohibition on general warrants—extend to the content of electronic communications like emails, *see, e.g., Vista Marketing, LLC v. Burkett*, 812 F.3d 954, 969 (11th Cir. 2016)

(citing *United States v. Warshak*, 631 F.3d 266, 268 (6th Cir. 2010)) ("the Fourth Amendment demands that the government demonstrate probable cause . . . to review the content of stored electronic communications"); and that, in this digital age, electronic communications like emails may be used for sharing and storing highly personal and sensitive information relating to the account holder and those with whom he or she communicates electronically.

In recent years, courts have begun grappling with how to balance the Government's legitimate interest in searching for evidence of alleged crimes that might be found in electronic communications like emails with the privacy rights of the email account user and those with whom the user has communicated. The practical realities of how potentially vast amounts of data may be collected, stored, transferred, and reviewed have made this balancing a difficult task. The Government's warrant applications in this case are not unique; they appear to track the Department of Justice's format for search warrant applications that has been reviewed in numerous published district court opinions in recent years. Of course, while some of these decisions have rejected applications like those presented here, one may safely presume that substantially more courts have approved of these applications, and issued search warrants, than have denied them. Nevertheless, for the reasons that follow, in this instance, the undersigned finds the applications before the court sufficiently problematic to join those courts that have rejected similar applications.[2]

---

[2] In particular, the court has found the reasoning and analysis set out in the following opinions rejecting similar search warrant applications to be particularly persuasive in analyzing the instant

As set forth in the above excerpt from the Government's applications, the Government's search warrants would require the disclosure to the Government of essentially all data, including the contents of communications, relating to the subject email accounts, without limitation as to time. After some method of review that the Government does not describe in any appreciable form, from this universe of data the Government will "seize" only what it considers "fruits, evidence, and instrumentalities" of the crimes that it is investigating "since January 1, 2015." There is no protocol requiring the destruction, discarding, return, or quarantining of data that the Government does not "seize." In the undersigned's view, these aspects of the Government's applications—that the Government's collection of data is not temporally limited despite its temporally-limited showing of probable cause (and its manifest intent to only seize evidence of specific crimes "since January 1, 2015"), and that the Government will keep and retain access indefinitely to all nonpertinent data it receives—render the Government's applications requests for unconstitutionally overbroad, general warrants.

As a preliminary matter, the undersigned notes that, irrespective of the concern articulated above, the validity of the Government's applications rests on the artifice that there is a distinction between what is disclosed to, and apparently kept by, the Government,

---

warrant applications: *In the Matter of the Search of premises known as: Three Hotmail Email accounts: [redacted]@hotmail.com, [redacted]@hotmail.com, [redacted]@hotmail.com Belonging to and Seized from [redacted]*, 2016 WL 1239916 (D. Kan. Mar. 28, 2016), *reversed in-part*, 212 F. Supp. 3d 1023 (D. Kan. 2016); *In re: [REDACTED]@gmail.com*, 25 F. Supp. 3d 1100 (N.D. Cal. 2014); and *In the Matter of the Search of Info. Associated with [redacted]@mac.com that is Stored at Premises Controlled by Apple, Inc.*, 25 F. Supp. 3d 1 (D. D.C. 2014).

and what the Government actually "seizes." In the undersigned's view, where an ECSP is compelled to "disclose" data, and where the Government intends to search through and keep all such disclosed data regardless of relevance, there can be no doubt that all data encompassed by the warrant is effectively seized. *See, e.g., In the Matter of the Search of Info.*, 25 F. Supp. 3d at 6-7; *In the Matter of the Search of Premises*, 2016 WL 1239916, at *12. This is so regardless of the fact that the Government purports to "seize" only a more narrowly defined subset of the data disclosed to it.

The undersigned recognizes those court opinions indulging the Government in this fiction and concluding that this "seize then search" methodology is permitted under Rule 41 of the Federal Rules of Criminal Procedure and the Stored Communications Act. *See, e.g., In the Matter of Search of Info. Associated with Email Addresses Stored at Premises Controlled by the Microsoft Corporation*, 212 F. Supp. 1023, 1034-37 (D. Kan. 2016) (reversing in-part the Magistrate Judge's opinion denying warrant applications); *In the Matter of a Warrant for All Content and Other Info. Associated with the Email Account xxxxxxx@gmail.com Maintained at Premises Controlled by Google, Inc.*, 33 F. Supp. 3d 386, 390-94 (S.D. N.Y. 2014) (granting search warrant). Although generally uncomfortable with that conclusion as a matter of law, the undersigned does not rest this Order on a rejection of that legal premise. Rather, the undersigned only discusses the legal fiction central to the Government's requests in order to lend context to the discussion of Fourth Amendment reasonableness to follow. That is, where the legality of the Government's conduct already depends upon an attenuated construction of what

constitutes a seizure, the court should be particularly scrupulous in holding the Government to its burden to show that its conduct is reasonable.

"[R]easonableness is always the touchstone of Fourth Amendment analysis[.]" *Birchfield v. North Dakota*, 136 S.Ct. 2160, 2186 (2016). In the search and seizure context, reasonableness is measured "by assessing, on the one hand, the degree to which it intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate government interests." *Wyoming v. Houghton*, 526 U.S. 295, 300 (1999). Here, the intrusion on the email users' privacy is substantial: every significant detail relating to the email account, including the content of every communication ever sent or received, is to be provided to the Government for inspection on terms and conditions known only to the Government, and to be retained by the Government indefinitely with no manifest restriction on the Government's ability to repeatedly review the contents of all email communications. Despite the Government's assurance that it will only "seize"—meaning, apparently, segregate from other seized data for the purposes of "use" in the investigation—evidence related to the crimes it is investigating "since January 1, 2015," there is no restriction on the Government's ability to take "plain view" of material that is not pertinent to its current investigation but that might be relevant to some other criminal investigation for which the Government has not presented probable cause to search for evidence.

So, then, one side of the required reasonableness balancing is substantially weighted. However, the undersigned must weigh against the Government's intrusion the

degree to which such intrusion is "needed for the promotion of legitimate government interests." *Houghton*, 526 U.S. at 300. Although the undersigned concedes that the Government has presented probable cause to believe that persons using the subject email accounts have participated to some degree in an identity theft scheme, and therefore some intrusion is warranted, the warrant applications do not explain, and the undersigned cannot fathom, why the absolute intrusion the Government seeks is needed. As noted previously, despite that it seeks disclosure of the contents of all communications to or from each subject email account, by its own terms, the Government seeks to "seize" only information constituting "fruits, evidence and instrumentalities" of certain crimes "since January 1, 2015[.]" In view of this definitive temporal limitation on what the Government ostensibly wants, the warrant applications fail to provide a sufficient justification for the overseizure[3] sought by the Government and described in this Order.

Furthermore, apart from the Government's own temporal limitation, the actual probable cause articulated with respect to each subject email address does not support the comprehensive disclosure sought by the Government. It is important to note at this juncture that, with fifteen different email accounts at issue, the Government's showing of probable cause naturally falls along a continuum of strength depending upon the extent of the involvement of each account. Each warrant application broadly describes the identity

[3] For clarity, the undersigned again emphasizes that, in this context, "seizure" refers to what the Government intends to collect and retain in its possession, not simply what the warrant itself describes as a seizure.

theft scheme and then describes some communications to or from the subject email account indicating that the email account was used to further the scheme. Some email accounts appear extensively involved.[4] Others appear much less involved. Indeed, one email account is described only as having received two emails and sent one email within a five-minute span one morning in February of 2017. *See* Ex. 7. Do three possibly incriminating emails spaced over five minutes one morning in 2017, supposedly in furtherance of an identity theft scheme beginning in 2015, justify the wholesale disclosure and unfettered inspection and retention of every email ever sent or received by that email account, no matter how many years prior to 2017 or 2015 such emails might have originated? If the Government can make the case that such overseizure is needed—not just desired, but *needed*—for the promotion of its interest in investigating a criminal scheme beginning in 2015, then the application before the court does not make it. Thus, it seems to the undersigned that, at this time, a reasonable balancing of the competing interests involved would permit the Government to search email content in closer temporal proximity to both the alleged criminal activity and, in particular, the email transmissions that the Government relies upon as establishing probable cause.[5]

---

[4] For example, a few email accounts are described as having exchanged dozens of emails over more than a year containing information in furtherance of the identify theft scheme.

[5] Judge Waxse's analogy is apt:

> The Court remains concerned that each of the target email accounts may—and likely do—contain large numbers of emails and files unrelated to the alleged crimes being investigated and/or for which the government has no probable cause to search or seize. . . . [T]hese warrants are akin to a warrant asking the post office to

The Government could easily strike a reasonable balance by, for example, limiting the "Information to be disclosed" in part 1.a of Attachment B of each of the proposed search warrants to "[t]he contents of all emails associated with the account *occurring after December 31, 2014*." By doing so, the Government would vindicate its interest in discerning the extent of the account user's involvement in the criminal activity under investigation without significantly prejudicing its stated objective to "seize" the "fruits evidence and instrumentalities" of certain crimes "since January 1, 2015." Perhaps a review of the content of emails occurring after 2014 would even uncover probable cause to justify a search into earlier emails, and would therefore warrant returning to the court to seek a second, broader search warrant. But there is no doubt that such a restriction would, as much as is reasonably practicable at this time, limit the Government's intrusion on the account user's expectation of privacy in their email communications. Thus, because the Government seeks at the outset to access and search potentially so much more than its specific showing of probable cause would support, the undersigned is left with the abiding conviction that what the Government actually seeks is "a general, exploratory rummaging,"

> provide copies of all mail ever sent by or delivered to a certain address so that the government can open and read all the mail to find out whether it constitutes fruits, evidence or instrumentality of a crime. The Fourth Amendment would not allow such a warrant and should therefore not permit a similarly overly broad warrant just because the information sought is in electronic form rather than on paper.

In the Matter of the Search of Premises Known as: Three Hotmail Accounts, 2016 WL 1239916, at *13 (quotation omitted). In other words, the mere fact that technological innovation has made such a seizure possible (or convenient) does not mean that the Fourth Amendment should now be enfeebled to accommodate it.

Coolidge, 403 U.S. at 467, through the content of all of the account users' email. The Fourth Amendment must require a stronger showing by the Government to permit intrusion of that magnitude.

In addition to concern about the overbreadth of the requested search warrants, the undersigned is concerned about the lack of any protocol for the Government's handling of non-pertinent information that the Government would compel the ECSP to disclose but that it ostensibly does not "seize." The warrant applications do not indicate that such information will be returned to the ECSP, destroyed, segregated, or quarantined from Government investigators. The Government's ability to repeatedly cull through potentially troves of highly personal—but ultimately irrelevant—information about the account users effects a continued violation of the account users' expectations of privacy for which no reasonable justification can be found in the application. This flaw is especially problematic considering that, as discussed previously, the Government seeks to compel the ECSPs to provide essentially every bit of data pertaining to the subject email accounts, without any limitation as to time or pertinence to its investigation.

The defects described in this Order present substantial jeopardy to the Fourth Amendment rights of the users of the email accounts targeted by the Government. The warrant applications fail to provide a sufficient basis for finding the defects reasonably necessary to promote the Government's interests in conducting its investigation. Moreover, it appears to the undersigned that the defects are either easily avoided or remediated. As such, the undersigned is compelled to find that these defects are fatal to

the Government's applications, and that such applications must therefore be denied at this time.

III. CONCLUSION

For all of the foregoing reasons, the undersigned DENIES the fifteen applications for search warrants related to the email accounts described in the applications presented to the undersigned on June 15, 2017.

DONE this 14th day of July, 2017.

/s/ Wallace Capel, Jr.
CHIEF UNITED STATES MAGISTRATE JUDGE

SUPERIOR COURT OF THE DISTRICT OF COLUMBIA

CRIMINAL DIVISION – FELONY BRANCH

In the Matter of the Search of www.disruptj20.org that Is Stored at Premises Owned, Maintained, Controlled, or Operated by DreamHost	**)**	**Special Proceeding No. 17 CSW 3438**
	)	**Judge Leibovitz**
	)	**Hearing: 9:30 a.m. Friday, Aug. 18, 2017**

DECLARATION OF KARL FRY IN SUPPORT OF DREAMHOST'S RESPONSE IN OPPOSITION TO UNITED STATES' MOTION TO SHOW CAUSE

I, KARL FRY, declare, under penalty of perjury as follows:

1. I am employed as a Compliance Analyst by DreamHost, LLC ("DreamHost"). In connection with my employment, I am familiar with the website www.disruptj20.org ("Website") and the data possessed by DreamHost in connection with DreamHost's hosting of the Website.

2. The information currently possessed by DreamHost pertaining to the Website is maintained in Oregon.

3. The Website promotes several e-mail addresses using the disruptj20.org domain name and invites correspondence. Each of the accounts for the email addresses are assigned to a different user and each account contains a separate login password.

4. HTTP logs contain extensive information about visitors to the website, including the time and date of the visit, the IP address for the visitor, the website pages viewed by the visitor (through their IP address), and even a detailed description of the software running in the visitor's computer. This information, together with information from the internet service provider for the IP address, would allow the government to identify the visitor to the website and the specific computers used to visit the website.

5. During the time period January 23, 2017 to January 28, 2017, DreamHost has maintained HTTP logs for over 1,300,000 IP addresses of visitors to the website.

6. DreamHost maintains e-mails associated with the Website, including emails of third parties, which are requested by Search Warrant.

7. DreamHost maintains membership lists for several e-mail discussion lists, from a number of different email accounts sponsored by the website. These discussion lists consist of groups of individual e-mail addresses.

8. DreamHost maintains over 2,000 images related to the Website.

9. The Website disseminates the data it publishes through DreamHost, to include press releases, messages, photographs, and other images, to the public.

10. Much of the information in possession of DreamHost was published to the public through the Website. Yet, other material, to include numerous draft blog posts, hundreds of images, including metadata for the images via detailed "datafields" that include titles and explanations for the images, do not appear to have been previously published.

11. The unpublished material appear to be similar to the material that were previously published. It is difficult to determine if the apparent unpublished material are preserved for a future publication date, or if the creator of the material previously excluded such material from publication. Some of the apparent unpublished material referenced above appears to be created after the day of the rioting incident.

12. The search warrant refers to, among other things, electronic "files, databases, and database records" to be seized. As I understand these terms, they cover every piece of electronic information possessed by DreamHost related to the Website.

13. Attached as Exhibit A is a true and correct copy of e-mails exchanged between the government and DreamHost and its counsel during the time period of July 14, 2017 through July 19, 2017.

I declare under penalty of perjury under the laws of the State of California that the foregoing is true and correct, and that this Declaration is executed on August 11, 2017 in Los Angeles, California.

/s/Karl Fry
Karl Fry

CERTIFICATE OF SERVICE

A true and correct copy of the foregoing was sent via e-mail and CaseFileXpress this 11th day of August, 2017, to:

AUSA John W. Borchert
U.S. Attorney's Office
555 Fourth Street, N.W.
Washington, D.C. 20530
john.borchert@usdoj.gov

/s/ Raymond O. Aghaian
Raymond O. Aghaian

From: "Christopher Ghazarian" <christopher.ghazarian@dreamhost.com>
Date: Jul 19, 2017 10:57 AM
Subject: Re: Search Warrant and Preservation (LGL-74338)
To: "Borchert, John (USADC)" <John.Borchert@usdoj.gov>
Cc: "legal@dreamhost.com" <legal@dreamhost.com>, "Kerkhoff, Jennifer (USADC)" <Jennifer.Kerkhoff@usdoj.gov>

Hi John,

DreamHost is having its annual “All Hands” meeting; the entire company gathers offsite for a day-long meeting, and we’re all out of the office in order to attend.

You asked Karl about producing the data immediately since it has been “preserved since January.” After reviewing the warrant, it looks like you are requesting *additional* data that wasn’t included in the preservations (“any messages, records, files, logs, or information that have been deleted but are still available to DreamHost….”). Thus, in order for us to comply with your warrant, Karl is pulling all of the new information from our database.

We kindly request additional time to put together what you’re asking for once we’re back in the office, and we will have an update for you as soon as possible (likely tomorrow) with production information and instructions.

Best,

Chris Ghazarian | **General Counsel**
213.787.4401 | chris@dreamhost.com | chris.law
707 Wilshire Blvd, Suite 5050, Los Angeles, CA 90017

> On Jul 19, 2017, at 6:04 AM, Borchert, John (USADC) <John.Borchert@usdoj.gov> wrote:
>
> Hello, Karl -

Thanks for your response. I sent a courtesy copy of the warrant to you last week, and you've had the data preserved since January. Can you please provide the materials to us today? If not, we may need to seek relief from the Court.

Regards,

John

From: Karl Fry [mailto:karl.fry@dreamhost.com]
Sent: Tuesday, July 18, 2017 8:31 PM
To: Borchert, John (USADC) <JBorchert@usa.doj.gov>; legal@dreamhost.com
Cc: Kerkhoff, Jennifer (USADC) <JKerkhoff@usa.doj.gov>
Subject: Re: Search Warrant and Preservation (LGL-74338)

Hi John,

We are in receipt of the warrant that was served yesterday; thank you. We have quite a bit going on this week, but I will be in touch as soon as I have more information for you.

We do appreciate your patience in the meantime.

Sincerely,
Karl Fry
DreamHost Compliance Team
http://www.dreamhost.com

On 7/18/17 10:45 AM, Borchert, John (USADC) wrote:

> Hello, Karl –
>
> You were personally served by the FBI yesterday. Can you please make a production to us today?
>
> Regards,
>
> John
>
> John W. Borchert
> Deputy Chief -- Felony Major Crimes Trial Section
> Misdemeanor Trial Unit
> U.S. Attorney's Office for the
> District of Columbia

Desk: 202-252-7679 Mobile: 202-870-6071
john.borchert@usdoj.gov

From: Karl Fry [mailto:karl.fry@dreamhost.com]
Sent: Friday, July 14, 2017 7:56 PM
To: Borchert, John (USADC) <JBorchert@usa.doj.gov>; legal@dreamhost.com
Subject: Re: Search Warrant and Preservation (LGL-74338)

Hi John,

Just as a reminder -- DreamHost does not accept substituted service for production orders. We respectfully request that such orders be served either in person at our downtown Los Angeles location, or with our registered service agent CT Corporation. The addresses for both can be found on our website, here:

https://www.dreamhost.com/legal/government-requests/

If you already intend to serve in person as well, please disregard.

Thanks,
Karl Fry
DreamHost Compliance Team
http://www.dreamhost.com

On 7/14/17 1:49 PM, Borchert, John (USADC) wrote:

> Hello, Karl –
>
> I have attached a search warrant that we have obtained for the disruptj20 website. Our preservation for this account dates back to January 17. I am also attaching an additional preservation letter dated today. Please let me know if you have any questions.
>
> Regards,
>
> John
>
> John W. Borchert
> Deputy Chief -- Felony Major Crimes Trial Section
> Misdemeanor Trial Unit
> U.S. Attorney's Office for the

District of Columbia
Desk: 202-252-7679 Mobile: 202-870-6071
john.borchert@usdoj.gov

SUPERIOR COURT OF THE DISTRICT OF COLUMBIA

CRIMINAL DIVISION – FELONY BRANCH

In the Matter of the Search of www.disruptj20.org that Is Stored at Premises Owned, Maintained, Controlled, or Operated by DreamHost	)	**Special Proceeding No. 17 CSW 3438**
	)	**Judge Leibovitz**
	)	**Hearing: 9:30 a.m. Friday, Aug. 18, 2017**

[PROPOSED] ORDER DENYING UNITED STATES' MOTION FOR NON-PARTY DREAMHOST TO SHOW CAUSE

Having considered the United States' Motion for DeamHost to Show Cause and the Response in Opposition by Non-party DreamHost, LLC, and related oral argument, the Court hereby DENIES the government's motion.

IT IS SO ORDERED.

Dated: August ___, 2017

_____
LYNN LEIBOVITZ
D.C. SUPERIOR COURT ASSOCIATE JUDGE